DETECTING MALICIOUS NODE IN WIRELESS AD-HOC NETWORK

[1]ARPITA NIRANJAN, [2]L.B BHAGWAT

[1,2]PG student, Assistant Professor, MIT, Pune
E-mail: niranjan.arpita18@gmail.com,laxmi.bhagwat@mitpune.edu.in

Abstract- Mobile Ad-hoc Network (MANET) is collection of mobile node that communicate with each other through wireless link directly or rely on other nodes that also act as router. Each device (node) is allowed to move independently in any direction and is free to change their links with other node frequently. Because of limited transmission power of nodes several nodes are required in order to deliver a packet from a source to destination. The intermediate nodes may cause several problems like it can deny to forward the packet, can extract useful information from the packet or may modify the content of packet. Such nodes are referred as misbehaving nodes. Packet dropping attacks can be a significant problem when it comes to MANETs. Encryption, Decryption & authentication solution is not sufficient to protect the MANET from these types of attacks. Misbehaving nodes uses the network and its services but they don't cooperate with other nodes. Such nodes don't consume any energy such as CPU power or bandwidth for retransmitting the data of other nodes and reserve them for themselves .In this paper, we implement a novel scheme using combination of E-Nack & E-2ack scheme, which is an enhancement of both N-ack & 2-ack scheme and is expected to outperform both N-ack scheme & 2ack scheme in terms of packet delivery ratio and packet dropping rate. Live Network (Java) is used to implement the proposed scheme and compare it against N-ack & 2-ack scheme.

Index Terms- AACK, 2ACK, N-ACK, Misbehaving Nodes, Mobile Ad-hoc Network(MANET), Watchdog.

I. INTRODUCTION

Security of packets is one of the primary concern while developing MANET due to frequently changing topology and dynamic nature of MANET. Most of the routing protocol proposed tends to assume that no node is malicious and each node cooperate in order to forward the packet. Thus one misbehaving node can cause the breakdown of entire network. Packet dropping attacks is one of primary concern when it comes to MANET. We can broadly classify the reasons of dropping packets into two type unintended and intended misbehavior. Unintended misbehavior can be caused due to various reasons like congestion problem, node overloading or collision. The intended misbehavior is further classified into two types- selfish behavior and malicious misbehavior. Both the selfish and malicious nodes have same action but they differ in their intentions. They carry the routing control packets but do not forward the data packets in order to conserve their energy or network bandwidth. However their intentions differ selfish node extract the useful information from control packet while the malicious nodes main purpose is to disturb the network.In this paper we mainly refer to nodes that causes intended misbehaviour.

We can classify the proposed techniques to detect misbehaving nodes in MANET into three type namely 1) Reputation Based technique 2)Credit based Technique 3) Acknowledgement based technique.In Reputation based technique all the network nodes collectively detect and declare the suspicious node as misbehaving and later this information is propagated throughout the network.This technique includes Watchdog and Pathrater. Credit based technique provide incentives for nodes in order to faithfully perform network functions. Nodes get paid to provide function to other nodes Acknowlegment based techniques rely on reception of acknowlegment as a proof that the packet has been successfully forwarded.The couple of scheme included in this are 2ACK, N-ACK,AACK scheme.

II. LITERATURE SURVEY

A. Watchdog and Pathrater

One of the traditional schemes is Watchdog [1] [2] that is used to detect the misbehaving node by overhearing the transmission. It was originally developed by Marti et al and was built on top of Dynamic Source Routing (DSR) protocol. It detects the misbehaving node by promiscuously listening to the next nodes transmissions. If the node fails to hear the transmission of next node then it increments that node failure counters. If the counter exceeds a certain threshold value then that node is marked as misbehaving node. Basically Watchdog detects the misbehaving node in network while Pathrater helps the routing protocol to respond to misbehaving node by avoiding such nodes in any future transmission. Advantage of this scheme is that it helps to identify the misbehaving node at forwarding level instead of just at link level. The major disadvantages of Watchdog scheme are: 1) Ambiguous collisions 2) Receiver collision 3) Limited transmission power 4) False misbehaviour report 5) Partial dropping.

In ambiguous collisions, the collision at node X prevents node X from overhearing the transmission of

Packet 1 from node Y to Z, due to Packet send to node X by S as shown in figure1

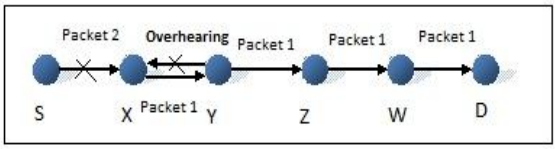


Figure 1. Ambigious collision

In receiver collisions, node X overhear the transmission of Packet1 from node Y to Z, but fails to detect that node Z don't receive that Packet1 due to collision with Packet2 at node Z, as shown in figure 2.

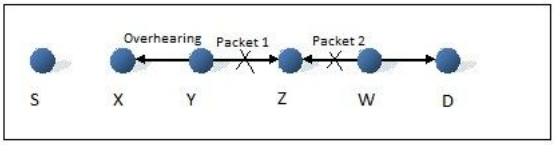


Figure 2. Receiver collision

In limited transmission power, node Y limits its transmission power in such a way that it is strong enough to be overheard by node X but too week for node Z to receive any packet, as shown in figure 3.

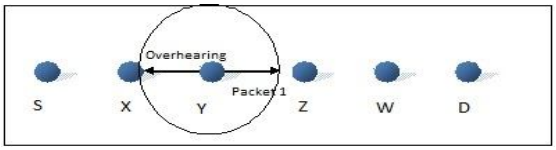


Figure 3. Limited transmission power

In false misbehaving report, although node X successfully overhears the transmission of Packet1 from node Y to Z , but node X itself misbehaves and falsely report node Y as misbehaving, as shown in figure 4.

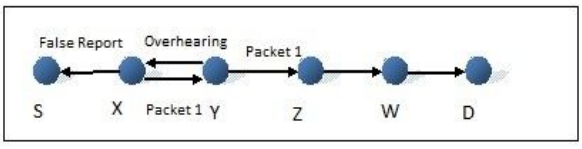


Figure 4. False misbehaviour report

B. 2ACK Scheme

Balakrishnan et.al proposed a new network layer scheme in order to overcome two major drawback of Watchdog scheme , collision and limited transmission power.It can be implemented at top of source routing protocol like DSR.TWOACK scheme [3] [4] is basically used to detect link misbehaviour instead of node misbehaviour.When a node sends a packet it verifies that the node at two hop distance along the route sucessfully receives that packet.This is achieved by special type of acknowledgment packet known as 2ACK which is send back in opposite direction for transmission. So every third node along the route is required to send back a 2ACK back to the first node within a time limit. If the node donot receives the 2ACK packet within time then it increment the nodes failure counter and if counter exceeds a threshold value then node is marked as malicious node.

As in figure 5,node X sends Packet1 to node Y which is successfully forwarded to node Z, so node Z is required to generate 2ACK packet and send it back to node X. The same process is repeated for every three consecutive node along the route.

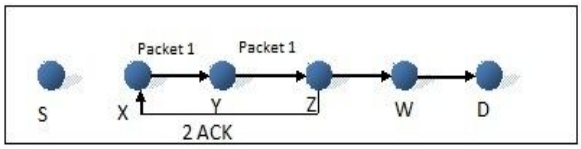


Figure 5. TWOACK scheme

C. N-ACK Schme

N-ACK scheme [5] is an extension of 2ACK scheme used to detect the malicious node in MANET environment.In this scheme an end to end Ack packet need to be send between source and destination.On reception of data packet the destination is required to send back Nack packet back to the source in the opposite direction in which intial data packet transmission take place.Each node maintains a list of data packet sent and data packt forwarded.As soon as source sends a packet it add the id of the packet to the list of data packet sent and will remove the id after the reception of Nack packet from the destination, otherwise id will be removed after the time out. The data packet and Nack packet both keep the track of route travelled.

If any node is found to be misbehaving in pre calculated route then intermediate node are provided with the provision that it can divert the Nack packet to reach the destination. Both route, the pre-calculated one and the new one is stored in Nack packet. The source on reception of Nack packet compares the two path, if they are found to be different then the node from which the path is found to be different is suspected as malicious node, if both the path are same then the source concludes that there are no malicious node along the path. For each node a threshold is maintained and if a particular node is found to be misbehaving more than its threshold value then it is marked as malicious node and this information is sent to all the neighbouring advising them that a particular node is misbehaving.

Also an additional provision is made where each node is required to send back a normal ack back to the immediate source after reception of data packet. This would help the immediate node to be aware if any its immediate neighbouring node is misbehaving or not and accordingly convey the information to other nodes

in network. It marks the immediate node as suspected node if it don't receive an ack within an preset time, if the no of time that node is suspected as malicious node exceeds a certain threshold value then its immediate source node marks that node as malicious node and convey the information to all the nodes in the network.

D. AACK Scheme

AACK scheme [6] [7] is a combination of Enhanced 2ACK scheme and end to end acknowledgment scheme.It aims to enhance the performance of 2ACK scheme. End to End acknowledgment scheme reduces the routing overhead in path with more than two hops as compared to 2ACK scheme.One of the major drawback of 2ACK scheme , that it fails to detect exactly which node is misbehaving is aimed to be overcomed with the help of AACK scheme.This is achieved by enhancing the 2ACK procedure.Due to combination of two scheme it helps to reduce the routing overhead and also enhances the detection efficiency.

1) Switching Scheme:-

AACK scheme basically works in two mode i.e. AACK mode and TACK mode. In AACK mode the system works as end to end acknowledgment scheme and In TACK mode the system will as E-2ACK scheme. As each node works in two modes so we need a switching system to switch between two modes. Default mode is AACK mode. The sender works in this mode until it encounters a timeout.

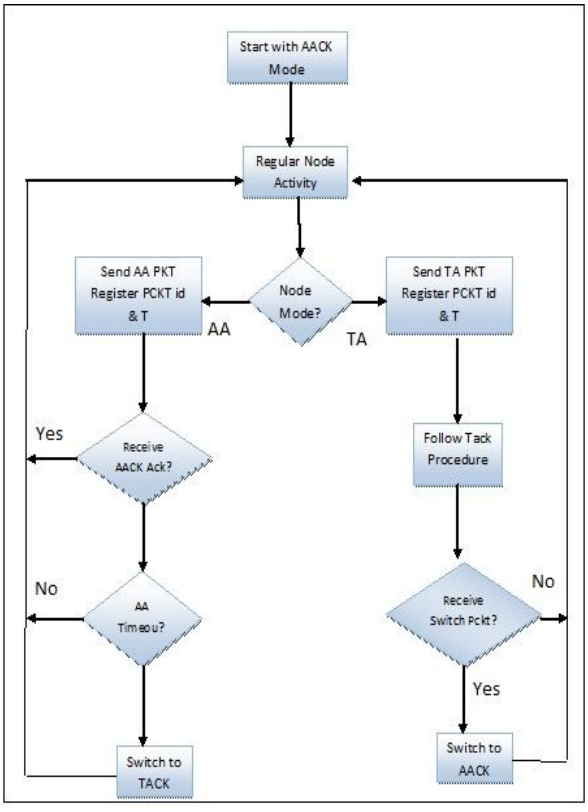


Figure 6. Switching scheme of AACK scheme

Table 1. Prons & Cons of Existing Systems

Sr. no	SCHEMES DISCUSSED	PRONS	CONS
1	WATCHDOG	Detects misbehaving node at forwarding level	)Ambiguous collisions Receiver collision)Limited transmission power)False misbehavior report)Partial dropping.
2	2-ACK	)Reliable data transmission)Reliable route discovery)Solves the problem:- collision and limited transmission power of Watchdog scheme	)Cannot detect exactly which node is misbehaving)Fails to detect the misbehaving node in case of false misbehavior report)Routing overhead.
3	N-ACK	Greatly reduces the overhead as compared to 2ack scheme	Fails to detect the malicious node in case of false misbehavior report.
4	AACK	Greatly reduces the acknowledgment overhead for large network Outperform the 2ACK scheme in terms of routing overhead & end to end delay	2ACK scheme has better performance than AACK because of switching overhead of AACK scheme.

III. IMPLEMENTATION OF PROPOSED SCHEME

A. E-Nack Description

The E-Nack scheme is an enhancement of N-ack scheme in order to detect the misbehaving node in MANET. The E-Nack scheme is required to send back Nack packet from destination to source after the destination receives the data packet.Each node is required to maintain a list of data packet sent and data packets forwarded. When a source needs to send a packet to a destination , it marks all the intermediate nodes including the destination as misbehaving node and sets up a timer for each of intermediate nodes in order to receive the ack from them. The source and each of the intermediate node is also required to sets up a timer for receiving N-ack packet from the destination.

As soon as the source sends a packet it add the id of the packet to the list of data packet sent,and each intermediate node adds it to the list of data packet forwarded. As each node recieves the N-ack packet for the data packet, the corresponding node will remove the remove the id of packet otherwise it will be removed after the time out.

Each intermediate node is required to send back an normal ack to source for each data packet is receive. If the ack is received by the source before time out then it mark the corresponding node as well behaved node otherwise it consider that node to be misbehaving.This would help the source to immediately detect which node is misbehaving at the forwarding level. With this scenario as there is no provision of third party(node) that can send can a false report about a node that is well behaved.

The data packet and N-ack packet keep track of route it travels. The Nack packet is required to reach the source in the same path in which the initial transmission takes place which it can retrieve from the data packet. However if any node misbehave in pre-calculated route then the intermediate nodes are free to divert the N-ack packet to reach destination. The source compares the two route , if they are same they source assumes that no node is misbehaving , if not then the node from where the path varies is assumed to be misbehaving.

For each node a threshold is maintained, if number of times a node is detected as misbehaving exceeds the threshold then the node is marked as misbehaving and information is sent to all the neighouring nodes. If the Nack packet is lost due to misbehaving or some other reason then the source will switch to E-2ack scheme in order to detect which node is misbehaving the the route.

B. Algorithm for E-Nack Scheme

Step 1:-Let Ni denotes the number of nodes in a particular route, where 1<=i<=k , and Let Ni be source that has to send a packet to the destination Nk via Nj, where 1<=j<(k-1).
Step 2:- Initially mark all the nodes in the route except the source as misbehaving node.
Step 3:- Set up timer for each of these individual node and wait for Ack.
Step 4:- Forward the packet to the consecutive node.
Step 5:- Add the id of the packet to the corresponding wait list.
Step 6:- While (Time for each node<= Threshold value)
If (Ack recv)
Then mark the node as well behaved node.
Else
If (Ack not recv and attempt <=n)
Resend the packet.
Else
Mark the node as misbehaving.
Step 7:- Repeat Step 4, 5 and 6.
Until (Nk receives the data packet)
Step 8:- Nk send N-ack packet back to Ni.
Step 9:- Each intermediate node Nj forward the N ack packet to the source Ni in the same path in which the initial transmission took place.
Step 10:- Each intermediate node ie Nj, also sets up a timer for arrival of N-ack packet.
Step 11:- If (Time<= threshold value and N-ack packet is recv)
Then remove the id of packet from corresponding wait list
Else
ID will be removed after Timeout.
Step 12:- Stop

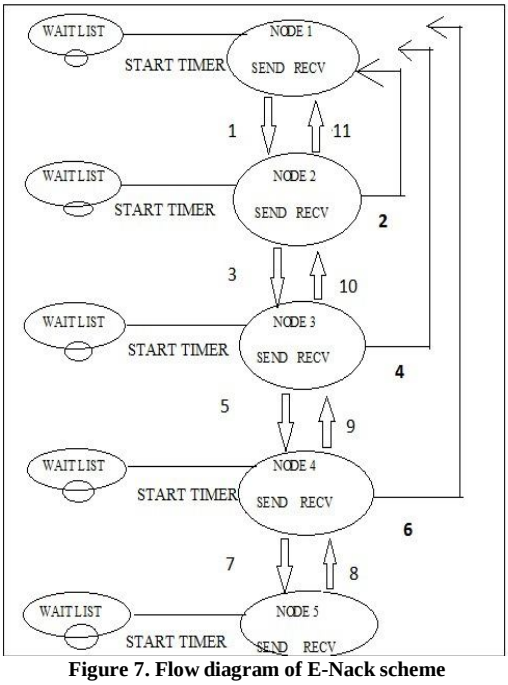


Figure 7. Flow diagram of E-Nack scheme

C. E-2ack Description

It is an enhancement of existing 2ack scheme which exactly detects which node is misbehaving in the triplet. From the nature of packet dropping attacks we can say that malicious node is one of the intermediate nodes and the destination node is excluded from this.

We use this in order to detect the exactly which node is misbehaving in the link. We can classify the node in three types: - Source(S), Forwarder (F) and Destination (D).

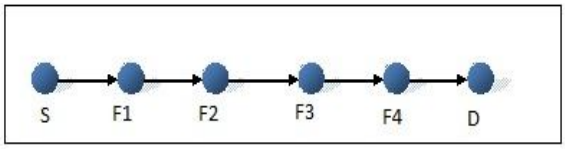


Figure 8. Path node types(Source, Forwarder,Destination)

There are four possibilities for a triplet:-

1. S-F-D (source, forwarder then destination).
2. F1-F2-D (forwarder, forwarder then destination).
3. F1-F2-F3 (forwarder, forwarder then forwarder).
4. S-F1-F2 (source, forwarder then forwarder).

In the traditional 2ack scheme, if the first in the triplet ie S or F1 does not receive a 2ack packet from the third node then it will report the link F-D, F2-D, F2-F3 and F1-F2 as misbehaving link. The E-2ack scheme will detect exactly which node is malicious in triplet:-

1. In (1) (2) the first node in the triplet i.e. S and F1 will report that the node just before the destination is misbehaving i.e. F and F2 will be reported as malicious.

2. In (3) the node F3 will be marked as malicious as a node before F1 has assured that link F1-F2 is well behaved as it has received a 2 ack packet from F2 so F3 will be the node that is misbehaving.

3. In (4) if F1 will misbehave then S won't receive 2ack packet or alarm from F2 and F1 respectively.

On the other hand if F2 is malicious node then F1 won't receive a 2ack packet from the node after F2 so it will send an alarm to F1 that F2 is misbehaving.

D. Switching Scheme

Each sender node needs to work in two mode:- E-Nack and E-2ack mode so a switching scheme is required in order to work in these two mode.

The default mode is E-Nack mode and the node works in this mode until it encounters a time out for the same.

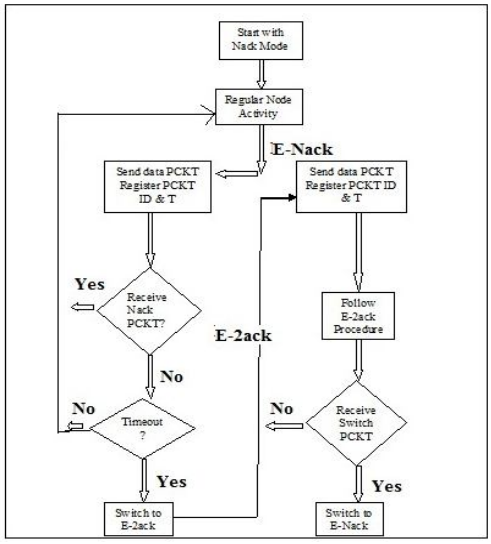


Figure 9. Switching Scheme for proposed scheme

E. Mathematical Model

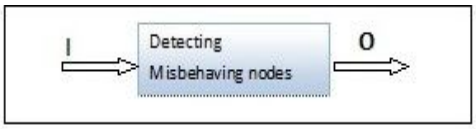


Figure 10. Mathematical model of the proposed system

Relevant Mathematics associated with the project:
Let System be S=(I,O,F,□)
Where,

I:Set of Inputs (Data Set)
1) Input to our system will be a graph G(V,E); such that
V= set of vertices and (1<=V<=N), where N is no of nodes in a particular route to destination
E= set of edges such that sum of weights of the edges in minimum i.e min(sum of wi), where wi are weight assigned to each edge.
2)Set of all possible paths between any two vertices V1 and V2 such that(V1, V2€ V) in graph G
O:Set of Outputs(Result Set)
1) Output will be the node or vertices which is misbehaving
2) Graph representing network overhead , packet dropping rate , packet delivery ratio and average end to end delay of the proposed scheme.

F :Set of Functions
Let function F be Fn=Fn1, Fn2....Fnn performed on the input to transform it into desired output.
1) Fn1=E-Nack Scheme
2) Fn2=E-2ack Scheme
□:Set of Constraints
□={□1,□2,□3}, where

□1= The proposed scheme can detect selfish node only when they do not work in group.

2=We have fixed topology (chain topology) in proposed scheme.

3=It only detects the node that causes intended misbehaviour not the one that causes unintended misbehaviour.

IV. RESULTS

In this paper we are implementing the proposed scheme in live network using java language. Initially we have implemented the N-ack scheme over a network of 5 nodes and have plotted the graph of routing overhead. Further we are planning to implement the proposed scheme i.e. combination of E-Nack & E-2ack scheme in live network in a network of approx 20 nodes

A. Results Obtained Without Malicious Node In Network



Figure 11. Transmission Of Packet from Node 1 to 3

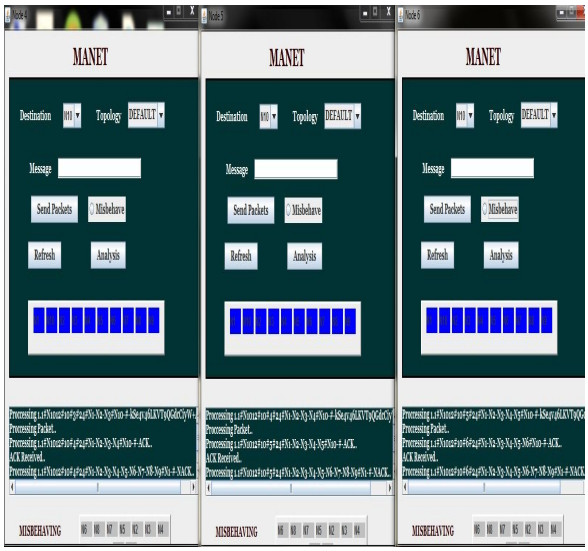


Figure 12. Transmission of Packet from Node 4 to 6

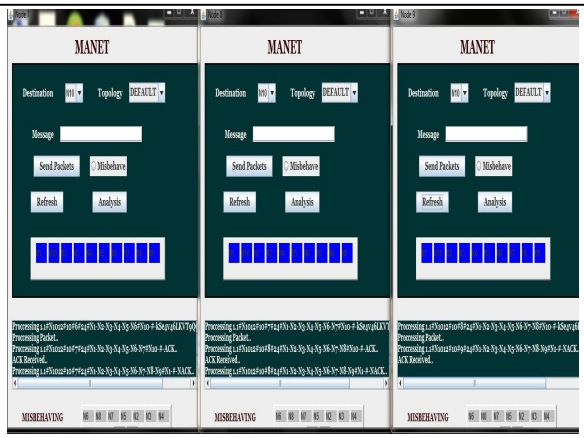


Figure 13.Transmission of Packet from Node 7 to 9

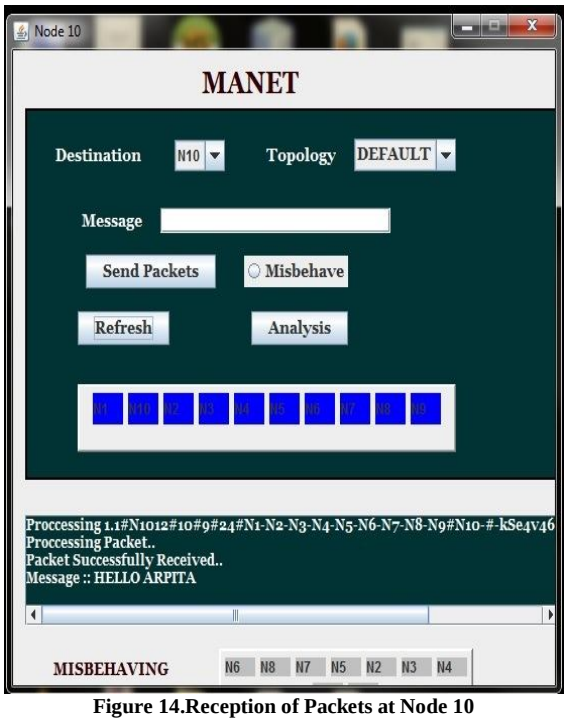


Figure 14.Reception of Packets at Node 10

B. Results Obtained With Malicious Node In Network(N6)

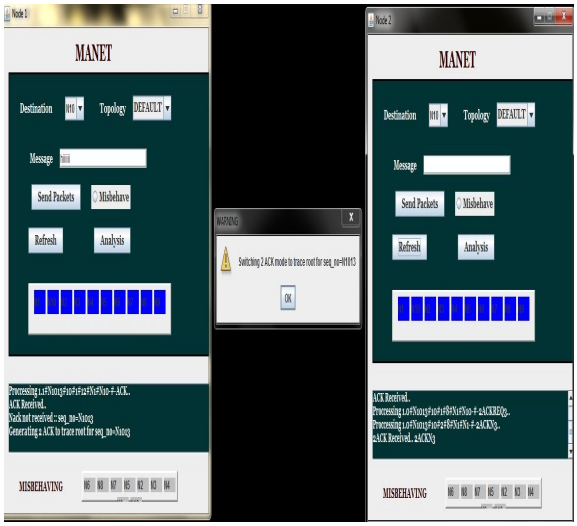


Figure 15. Transmission Of Packet from Node 1 to 2

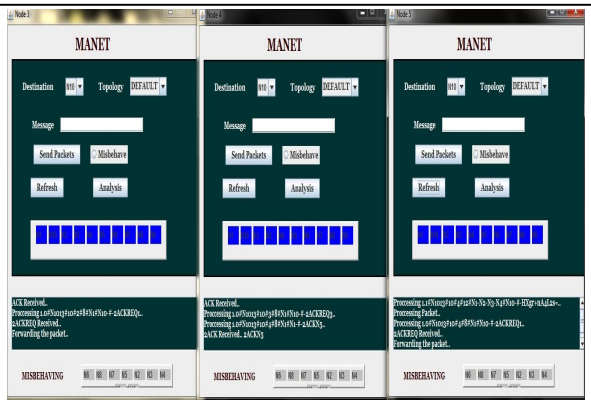


Figure 16. Transmission of Packet from Node 3 to 5

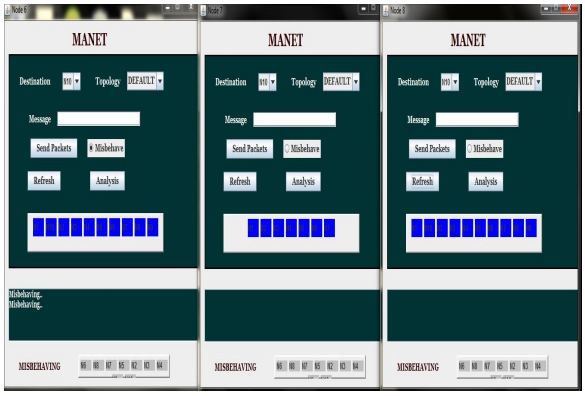


Figure 17. Detection of Misbehaving Node (N6)

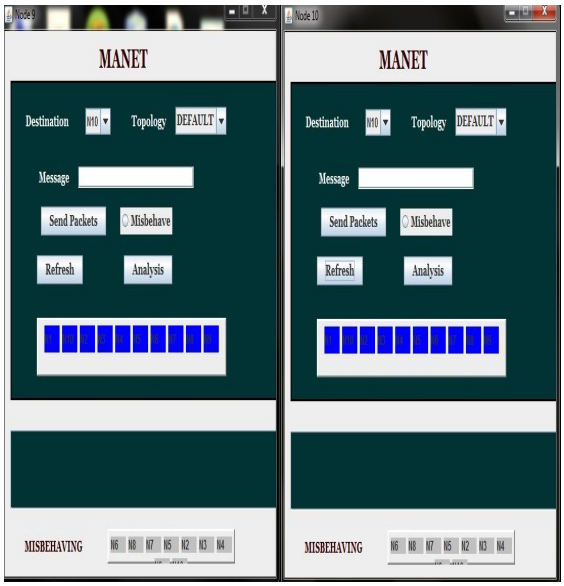


Figure 18.No Transmission of Packet to Node 9 and 10

CONCLUSION

Packet-dropping attack has been a major threat for the security in MANETs. To deal with this, a new novel approach, which is a combination of N-ACK Scheme and Enhanced TWO-ACK Scheme has been proposed in this paper. This scheme is expected to overcome the major drawbacks of existing systems (e.g. Watchdog, 2ACK) which are receiver collision, limited transmission power, and false misbehaviour report. The Proposed Scheme is also expected to outperform the traditional Schemes like Watchdog, 2ACK, N-ACK Scheme in terms of both packet delivery ratio and packet dropping ratio.

REFERENCES

[1] Sergio Marti, T.J Giuli, Kevin Lai and Mary Baker(Stanford university), “Migrating Routing Misbehaviour In Mobile Ad-Hoc Network",,ACM ,2000.

[2] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE "EAACK A Secure Intrusion-Detection System for MANETs "IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013..

[3] Sunilkumar S. Manvi, Lokesh B. Bhajantri, and Vittalkumar K. Vagga, "Routing Misbehaviour Detection in MANETs Using 2ACK", Journal of telecommunication and information technology (2010).

[4] Shirina Samreen and G. Narasimha, "An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehaviour",IEEE 2012

[5] S.Usha, Research Scholar and Dr. S.Radha Prof, ""Co operative approach to detect misbehaving nodes in MANETs using Multi-hop acknowledgement scheme", IEEE 2009

[6] Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", IEEE 2010.

[7] Ms.Sonali P. Botkar and Mrs. Shubhangi R. Chaudhary, "An Enhanced Intrusion detection System using Adaptive Acknowledgment based Algorithm", IEEE 2011.

[8] Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, "Detecting Misbehaving Nodes in MANETs", ACM 2010.

[9] U. Sharmila Begam1, Dr. G.Murugaboopathi, "A Recent Secure Intrution Detection System for MANET", International Journal of Emerging Technology An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013

[10] Nan Kang, Elhadi M.Shakshuki and Tarek R. Sheltami, "Detecting Forged Acknowledgements in MANETs, IEEE 2011.

★★★